KING COUNTY

SECURITY ENGINEER
INFORMATION SYSTEMS ANALYST IV
DEPARTMENT OF EXECUTIVE SERVICES
INFORMATION AND TELECOMMUNICATIONS SERVICES DIVISION
Annual Salary Range: $62,173 – $87,676
Job Announcement: 05CY5048
OPEN: 3/28/05 CLOSE: 4/8/05

WHO MAY APPLY: This position is open to the general public.

WHERE TO APPLY: Required application materials can be mailed to: **Christine Ynzunza, 700 Fifth Avenue, Suite 2300, Seattle, WA 98104, Fax 206-263-4834.** Email applications are encouraged at HRITS@metrokc.gov (all application materials must be included). Applications materials must be received by 4:30 p.m. on the closing date (Postmarks are NOT ACCEPTED.) ***PLEASE NOTE:*** Applications not received at the locations specified above and those that are not complete may not be processed.

***FORMS AND MATERIALS REQUIRED*:**

- King County application form. Application forms may be found at http://www.metrokc.gov/ohrm/jobs/JobApplications.htm
- Resume
- A letter of interest not to exceed two pages in length detailing your background and describing how you meet or exceed the requirements.

WORK LOCATION: 700 Fifth Avenue (Seattle Municipal Tower), Seattle, WA.

WORK SCHEDULE: This position is exempt from the provisions of the Fair Labor Standards Act, and is not overtime eligible. The workweek is normally Monday through Friday 8:00 a.m. to 5:00 p.m.

POSITION PURPOSE: This position will be responsible for analyzing information technology systems (LAN/WAN, operating systems, applications, desktop, data, integration) and deploying measures to safeguard the county against accidental or unauthorized modifications, denial, destruction, or disclosure. The County's Chief Information Security Officer (CISO) will focus on the formulation and administration of policies, standards, and guidelines at the County-wide level. This position is operationally focused on those domains under the purview of King County's enterprise technology service organization (Information and Telecommunications Services Division).

PRIMARY JOB DUTIES INCLUDE:

- Confer with management, risk assessment staff, the county's Chief Information Security Officer (CISO), external auditors, and other agencies as required to identify and plan security for data, applications and availability in networked installations.
- Proactively develop methods for implementing security practices in a networked environment.
- Oversee the planning, design, and implementation of appropriate information technology security tools.
- Implement appropriate monitoring and reporting tools. Review operation logs and event console activity to determine cause of security related events or to identify potential security related events. Recommend goals and objectives relative to security initiatives and report progress as required.

- Proactively protect the integrity, confidentiality, and availability of information technology resources by:
  - Responding in a timely manner to a loss or misuse of information technology assets
  - Participating in investigations of suspected information technology security misuse or in compliance reviews as requested by auditors
  - Communicating unresolved information technology security exposures, misuse, or noncompliance situations with management.
- Oversee the development and establishment of security procedures and vendor maintenance standards and ensure compliance for auditing and preventive maintenance purposes. Prepare and administer equipment service contracts with vendors as required.
- Identify problems, including security, disaster recovery/business continuity and privacy issues, and help create solutions, strategies and resource requirements to mitigate the problems.
- Assist with the review of security policies, and formulate internal operating procedures as required.
- Acts as a technical resource to information technology staff as required.
- Other duties as assigned.

QUALIFICATIONS:

In addition to a Bachelor's degree in Computer Science, Engineering, or related discipline or the equivalent combination of education and experience, the successful candidate will demonstrate a progression of increasingly responsible experience in the areas listed below:

- Three to six years of experience directly related to information technology security. This experience should include active participation in security programs and processes that have contributed to the development and administration of an organization wide IT security policy.
- Experience in LAN/WAN and multiplatform environments.
- Demonstrated competency in developing effective solutions to diverse and complex business problems.
- Strong analytical and problem-solving skills.
- Excellent oral and written communications skills.
- The ability to work effectively with others.
- The ability to present and discuss technical information in a way that establishes rapport, persuades others, and gains understanding.

DESIRED QUALIFICATIONS:

- Master's degree in information technology or MBA is preferred.
- Network Engineer or Systems Engineer certification is highly desirable.

SELECTION PROCESS: Competitive applicants will be invited to participate in an interview. Salary will depend on qualifications and availability of funds.

UNION REPRESENTATION: This position is not represented by a union.

CLASS CODE: **404700**